Amendments to the Claims

Please amend and add new claims as indicated below. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for utilizing a pseudonym for a permanent key pair, the method comprising:

producing [a] the pseudonym for the permanent key pair, the pseudonym including a public pseudonym key within a platform;

placing the public pseudonym key into a certificate template;

performing a hash operation on the certificate template to produce a certificate hash value;

performing a transformation on the certificate hash value for transmission from the platform;

receiving a signed result being a digital signature for the transformed certificate hash value; [and]

performing an inverse transformation on the signed result to recover a digital signature of the certificate hash value; and

erasing at least the public pseudonym key after utilization in a communication session.

2. (Original) The method of claim 1, wherein the producing of the pseudonym includes generating the public pseudonym key and a private pseudonym key corresponding to the public pseudonym key.

3. (Original) The method of claim 1, wherein the placing of the public pseudonym key into the certificate template includes writing the public pseudonym key into a field of the certificate template.

4. (Original) The method of claim 1, wherein the performing of the transformation comprises:

performing a logical operation on the certificate hash value using a pseudo-random number to produce a value differing from the certificate hash value.

5. (Original) The method of claim 4, wherein the pseudo-random number is a predetermined value raised to an inverse power designated by a pseudo-random value.

6. (Original) The method of claim 5, wherein the pseudo-random value is stored in secure memory.

7. (Original) The method of claim 4, wherein the performing of the inverse transformation comprises performing a logical operation on the signed result using an inverse of the pseudo-random number.

8. (Original) The method of claim 1, wherein prior to receiving the digital signature, the method comprises:

digitally signing a certification request, including the transformed certificate hash value, with a private key of a first platform to produce a signed certification request.

9. (Original) The method of claim 8, wherein prior to receiving the digital signature, the method further comprises:

obtaining a device certificate being a digital certificate chain that includes a public key of a first platform, to accompany the signed certificate request

10. (Original) The method of claim 9, wherein prior to receiving the digital signature, the method further comprises:

transferring the signed certificate request and the device certificate to a second platform.

11. (Previously Presented) The method of claim 1 further comprising:

storing the digital signature of the certificate hash value for use in subsequent communications to a remotely located platform.

12. (Previously Presented) A device comprising:

a processing unit; and

a persistent memory including a first key pair and at least one pseudonym for use in communications with a remotely located device and in identifying that a platform containing the device is secure, wherein the at least one pseudonym includes a second key pair that is erased after a communication session with the remotely located device has concluded.

13-14. (Cancelled)

15. (Original) The device of claim 12 further comprising:

a number generator to assist in producing the at least one pseudonym.

16. (Currently Amended) A platform comprising:

a transceiver; and

a device in communication with the transceiver, the device including a persistent memory to contain

a permanent key pair,

at least one pseudonym generated internally within the device and

a digital signature of a hash value of a digital certificate chain that includes a public pseudonym key of the at least one pseudonym, wherein at least the public pseudonym key is erased after utilization in a communication session.

17. (Original) The platform of claim 16, wherein the device further includes:

a processing unit to

(i) write the public pseudonym key into a certificate template,

(ii) perform a hash operation on the certificate template to produce a certificate hash value,

(iii) to perform a transformation operation on the certificate hash value.

18. (Original) The platform of claim 17, wherein the processing unit of the device further produces a digital signature of at least the transformed certificate hash value using a private key of the permanent key pair.

19. (Previously Presented) The platform of claim 17, wherein the processing unit of the device further appending a device certificate with the digital signature of at least the transformed certificate hash value.

20. (Original) The platform of claim 19, wherein the device certificate is the digital certificate chain.

21. (Original) A method for utilizing a persistent memory of a device, comprising:

storing in the persistent memory a first key pair; and

storing in the persistent memory at least one pseudonym for use in communications with a remotely located device and in identifying that a platform containing the device is secure, wherein the at least one pseudonym includes a second key pair that is erased after a communication session with the remotely located device has concluded.

22. (Original) The method of claim 21 further comprising:

utilizing a number generator to assist in producing the at least one pseudonym.

23. (New) A machine accessible medium having associated instructions for utilizing a persistent memory of a device, the instructions, when accessed, result in one or more machines performing:

storing in the persistent memory a first key pair; and

storing in the persistent memory at least one pseudonym for use in communications with a remotely located device and in identifying that a platform

containing the device is secure, wherein the at least one pseudonym includes a second key pair that is erased after a communication session with the remotely located device has concluded.

24. (New) The medium of claim 23, wherein the instructions include further instructions, which when accessed, result in the one or more machines performing:

utilizing a number generator to assist in producing the at least one pseudonym.